Strathmore
UNIVERSITY

THE LEGAL AND REGULATORY FRAMEWORK GOVERNING CYBERBULLYING AND HARASSMENT IN KENYA

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE BACHELORS OF LAWS DEGREE

KAMAU PETER NDUNG'U- 072475

STRATHMORE LAW SCHOOL

JANUARY 2016

CONTENTS

ACKNOWLEDGEMENTS

I would like to acknowledge my Project Supervisor Dr Isaac Rutenberg for his input and assistance in putting together this paper and the Strathmore Law School fraternity for imparting knowledge in me during my time in school.

Gratitude goes to both my parents for their invaluable and continued support during my undergraduate studies and my family in general for the support they gave me.

Most importantly, I would like to thank God for seeing me this far throughout my undergraduate studies and in undertaking this project.

DECLARATION

I hereby certify that this is my original work done in partial fulfilment of the requirements of the Bachelor of Laws degree in Strathmore University Law School. It has not been submitted to any other institution for any other qualification.

STUDENT

..... 31st March 2016

Kamau Peter Ndung'u Date

SUPERVISOR

..... 12/4/16

Dr. Isaac Rutenberg Date

DEDICATION

This paper is dedicated to all those affected by forms of online harassment and bullying with the hope that it will inspire change in the legislation to protect everyone's rights.

ABSTRACT

Cyberbullying and harassment is a developing phenomenon brought about by the development of the internet. Kenya is ranked 4th highest internet connected country in Africa with internet penetration levels of up to 28.6%. The development of the internet has led to positive outcomes such as improved communication but has also seen the rise of cybercrime. Cyberbullying is only a part of cybercrime with its nature being using information and communication technologies such as social media, email, blogs and websites to cause harm to others. In Kenya, this is on the rise and there is need to develop a working framework regulating against it. The freedom of expression theory may be used as an argument against these laws however, it is established that there are limitations to this freedom under the same Constitution that provides for it.

The current legislation consists of the Constitution of Kenya 2010, the Kenya Information and Communications Act and the Cybercrime and Computer Related Crimes Bill of 2014. None of these legislations apart from the Constitution which provides a general outline, deals directly with cyberbullying and harassment.

The paper uses qualitative research methodology deriving information from primary, secondary and tertiary sources most of these being journal articles, reports and statutes. It also draws comparisons from selected jurisdictions to provide an understanding of how various jurisdictions deal with cybercrime and harassment. This paper also finds that the framework regulating against cyberbullying and harassment is not adequate and needs to be improved on. Amendment of the Bill before its assent, institution of a specialised Cybercrimes Department in the Criminal Investigation Department of the Police and the D.P.P's office, Cyber Resource centres and education and awareness are some of the recommendations made by this paper.

LIST OF ABBREVIATIONS

C.A	Communications Authority
C.C.K	Communication Commission of Kenya
C.J.C.P	Centre for Justice and Crime Prevention
C.P.S	Crown Prosecution Service
D.P.P	Director of Public Prosecution
I.C.T	Information and Communications Technology
K.O.T	Kenyans On Twitter
O.D.P.P	Office of the Director of Public Prosecution
S.M.S	Short Message Service
T.C.R.A	Tanzania Communications Regulation Authority
U.K	United Kingdom

CHAPTER 1

1.1.BACKGROUND OF THE PROBLEM

The 21st century has seen the development and penetration of technology in Kenya and the world at large. As at November 2015, internet penetration rates showed that Africa has a 28.6% penetration.[1]This is a high percentage compared to other continents basing this on the fact that Africa is considered to be a developing continent. The focus on Africa puts Kenya at third position in the number of internet users with 32 million users after Nigeria and Egypt. This can be largely attributed to the growth of data services in Kenya with 21.5 million subscriptions for mobile data while wireless data subscriptions shows numbers at 13, 221 subscriptions while fixed data subscribers at 2,500. [2] These growing figures indicate a rise in internet usage locally, mainly attributed to increased availability of web enabled mobile phones. The internet is part of this development which has created a lot of opportunities and improvement, specifically to how people network and communicate. Kenyans are able to communicate virtually through various forms of new media such as email and social networks through computers and other forms of electronic communication.

Most Kenyans use the internet largely for social media and digital content with the majority of that age being 16-25. [3] This age group exposes itself to communication and interaction on social media sites like Facebook, Twitter and LinkedIn. Facebook has a big presence in Kenya, with almost 5 million users as at November 2015 [4] with twitter having close to 3 million users as at 2014[5]. These two social media sites largely form the biggest interaction on social media in Kenya.

Over the years, hate speech, libel, insolence, online bullying and harassment have cropped up. From the United States, the U.K to Africa, cyberbullying is rife and is affecting children and adults altogether. In Kenya, there is a growing need to have legislation

---

[1] http://www.internetworldstats.com/stats.htm on 5 January 2016.
[2] Communications Authority, 1st Quarter Sector Statistics Report for the Financial Year 2015-2016.
[3] UNICEF, *A (Private) Public Space Examining the Use and Impact of Digital and Social Media Among Adolescents In Kenya*(2013).
[4] http://www.internetworldstats.com/africa.htm#ke on 5 January 2016.
[5] http://www.moseskemibaro.com/2014/08/01/sizing-up-twitter-in-kenya/ on 5 January 2016.

governing online behaviour. The current legislation does not provide adequate law on cyberbullying or any form of online harassment such as stalking. As such, the incidents on cyberbullying especially on social media networks such as Facebook and Twitter are on the rise. Kenyans on Twitter or "#KOT" as they are famed, are very famous for backlash and group remonstration with users hiding behind anonymous usernames. There is a need to regulate online behaviour while taking regard to the fundamental freedoms and rights that are enshrined in the Constitution.[6]

1.1.0 Nature of Cyberbullying

Defining cyberbullying is somewhat of a task due to the variations involved. However, one certain fact is that it involves electronic means. Bill Belsey, an author from Canada who has been instrumental in developing the Canadian framework, proposes a working definition of cyberbullying. It involves the use of information and communication technologies like email, SMS, Instant Messaging, blogs, social media sites, online polling websites to support deliberate, repeated and hostile behaviour by an individual or a group with the intention of causing harm to others.[7] Kowalski notes that these are communication modalities through which it takes place. They include Instant messaging, electronic mail, text messaging, bash boards in chat rooms, social media sites such as Facebook and twitter, websites.[8] Cyberbullying affects children whereas cyber harassment affects adults. There is debate around this from different authors, however, this study will involve the two concurrently due to their close relationship. Several behaviours constitute cyberbullying. These behaviours may be harassment, impersonation, among others.[9]

1.2 STATEMENT OF THE PROBLEM

The problem in Kenya is that there is no regulatory framework governing online harassment of private persons in the country. This creates room for malice online, giving

---

[6] Chapter 4, *Constitution of Kenya* (2010).
[7] Bill Belsey, *Cyberbullying: An Emerging Threat to the "Always On" Generation* (Cochrane, Alta: Cyberbullying.ca, 2007) at 3 available at http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf on 5 December 2015.
[8] Robin M. Kowalski, Susan P. Limber, Patricia W. Agatston, *Cyberbullying: Bullying in the Digital Age* (2012) 56-118.
[9] Robin M. Kowalski, Susan P. Limber, Patricia W. Agatston, *Cyberbullying: Bullying in the Digital Age* (2012) 56-118.

people a chance to hide behind anonymity and participate in harassment in an unpoliced environment. This should not be the case as the same acts of harassment and bullying are punishable offline under law.

1.3 HYPOTHESIS

The hypothesis of this study is that the legal and regulatory framework in Kenya is inadequate to deal with cyberbullying and harassment.

1.4 JUSTIFICATION OF THE STUDY

According to the United States National Crime Prevention Council, Cyber bullying refers to harassment that occurs via the internet, cell phones or other devices that facilitate access to the internet. In this, communication technology is used to intentionally harm others through hostile behaviour online.[10] This is part of the dark side of technology. The study is informed by the development of social networking brought by the advancement of technology and the rising number of internet users. These numbers are multiplying every year with data becoming increasingly accessible and affordable to Kenyans almost every quarter of the year according to the Communications Authority Quarterly Sector Reports. Through online facades, people have been able to disrespect each other's rights and have created an environment for tortious liability on the frontiers of harassment. In Kenya, there has been a rise in indiscriminate social media bullying by people in online platforms such as Twitter (which is the most notorious) and Facebook. The current state of matters is that these victims have no information on how to tackle and prevent this. It is therefore important to address this matter now and for the future as cyberspace is hugely becoming a wide and ungoverned terrain needing proper regulation. This study will show that the laws in Kenya do not provide for adequate protection against cyberbullying and online harassment drawn from an analysis of the current framework and a comparison with other jurisdictions.

1.5 STATEMENT OF OBJECTIVES

The following objectives shall guide this study:

---

[10] http://definitions.uslegal.com/c/cyber-bullying/ on 27 September 2015.

1. Establishing the nature of cyber bullying in Kenya, how it occurs and where it occurs.

2. Analysing the current legislation on cyber bullying and online harassment.

3. Illustrate a need for improved legislation on cyber bullying and related offences in Kenya.

4. Propose recommendations on the scope of legislation that will create a regulatory framework for regulation of cyberbullying in Kenya.

1.6 RESEARCH METHODOLOGY

This study is founded on qualitative data from primary, secondary and tertiary sources including information analysis from journals, articles, books, statute law from both Kenya and outside Kenya and reports.

1.7 LIMITATIONS OF THE STUDY

This study is limited to the use of qualitative resources where is a general shortage of existing literature on the nature and extent of cyber bullying in Kenya. It is a relatively new problem that has been brought about by technological development and may rely on internet resources and comparative analysis from jurisdictions dealing with the problem appropriately.

1.8 CHAPTER SUMMARY

The paper is divided into five chapters. The first chapter consists of the background of the study, justification of the study, research objectives and limitations of the study. The second chapter includes the theoretical framework involved in answering the research questions. The third chapter consists of the Kenyan context detailing the current framework in place to address the problem being investigated. The fourth chapter consists of a comparative analysis between Kenya and three jurisdictions namely the United Kingdom, Tanzania and South Africa and discusses the findings of the analysis. The last chapter then proposes recommendations to addressing the problem and arrives at a conclusion to the study.

CHAPTER 2: THEORETICAL FRAMEWORK

Bullying and harassment have for years been common occurrences in society. Bullying is an age-old societal problem, beginning in the schools and subsequently progressing outside. Traditionally, bullying has existed in many circles, mostly rampant in schools. [11] However, over the years it has taken a new form and encroached in a space masked by anonymity of identity.

Some scholars indicate that this new form of bullying is only an extension of physical bullying and harassment and that it ought not to be treated differently from physical bullying while others argue that it is a new form with new adaptations hence presenting a new way to deal with it. Rodkin and Fisher contend that cyberbullying is ubiquitous, anonymous, extended in physical distance, hard to detect and of variable duration.[12] While this distinction exists, the dynamic of cyberbullying changes with the introduction of technology. Without technology, it is just bullying. This chapter proposes theories that seek to arrive at an answer to the research questions.

2.1 Freedom of Expression Theory

John Stuart Mill advocates for the freedom of expression alongside the freedom of thought. He suggests that there is required the fullest liberty of expression to push our arguments to their logical limits. Further, he advocates for the protection of free speech but also recognises that there can be exceptions to forms of expression that provide a positive instigation to mischievous acts. He places the limitation of this freedom on a principle known as the Harm Principle which holds that the actions of individuals should only be limited to prevent harm to other individuals.[13] This theory contends that the freedom of expression ought to be respected, however it is not an absolute freedom and that limitations must be made when harm is the subject of prevention.

---

[11] Campbell, Marilyn A (2005) Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling* 15(1):68-76.

[12] Philip C. Rodkin and Karla Fischer, Cyberbullying from Psychological and Legal Perspectives, Missouri Law Review Volume 77, Article 3 (619-640).

[13] John Stuart Mill, On Liberty, (1859) at 195 available at https://books.google.co.ke/books?id=qCQCAAAAQAAJ&dq=on+liberty&pg=PP1&prev=http://www.google.com/search%3Frlz%3D&q=On+Liberty&redir_esc=y#v=onepage&q=On%20Liberty&f=false on 9 January 2016.

Thomas Michael Scanlon on the other hand, proposes permissible justifications for legal limitations on expression. They include expression resulting to direct physical injury or damage, expression producing harmful or unpleasant state of mind, expression causing panic and expression causing others to form an adverse opinion or interference with rights.[14]

Cyberbullying and harassment can be argued to be the mere expression of an individual's freedoms. This theory, while advocating for the freedom of expression online and offline, also expresses certain limitations. The right to limiting the freedom of expression must meet certain criteria. These restrictions must be prescribed by law, must pursue a legitimate aim such as protection of morals [15]and must show necessity and a direct and immediate connection between the expression and the protected interest. The Kenyan Constitution also plays a key part in limitation of this freedom. [16]

Using this theory, if the occurrence of bullying and harassment offline results to harm as proposed by John Stuart Mills, then it should also be against the freedom of expression when it occurs online as the only difference is the use of technology to facilitate bullying and harassment online.

[14] "A Theory of Freedom of Expression," Philosophy and Public Affairs 1, No.2 (1972), 204-226.
[15] Article 19 (3)(a)(b), *International Covenant on Civil and Political Rights*, 16 December 1966.
[16] Article 24, *Constitution of Kenya* (2010).

CHAPTER 3: THE KENYAN CONTEXT

3.1 INTRODUCTION

The introduction and development of the internet in Kenya has received a huge welcome from the whole country at large. A good example of this would be the integration of the ICT ministry in Kenya and the incorporation of ICT in achieving Kenya's vision 2030 goals. The Draft ICT policy underwent review by the Ministry of ICT to ensure that a pro-active policy in sync with contemporary technological realities and dynamics was developed while recognizing the tremendous impact of globalization and the rapid changes of technology.[17] This was just among the many efforts to ensure that technology fosters development and creates a big impact in the country. With the main goal in sight, there have been efforts to create legislation surrounding the ICT and communications sector due to the dynamic rise and advancement of technology in Kenya. [18] The increasing stats on internet usage and penetration in the country have called for the realisation of the importance of an ICT policy in the country.

The internet presence is widely felt in Kenya and more so on social media channels. Social media usage in Kenya has been on a high and is attributed to be the main reason most Kenyans use the internet. Statistics indicate that of the 31 million internet users as at 2015, as estimated by the Communications Authority, 5 million of those users have Facebook accounts. [19] Statistics on twitter's usage and reach in Kenya have not been officially documented so far but estimations range from 1.4 million active users to the region of 2.5 million active users. [20] The two social media sites are the most widely used in Kenya. Though there is a large number of Kenyans on Whatsapp, it cannot be termed as a social media site but instead it is a cross platform mobile messaging app that allows people to exchange messages with each other.[21] Other social media sites such as Google Hangouts, Tumblr and YouTube enjoy a substantial audience in Kenya that may soon increase as time dwindles by.

---

[17] Foreword, *ICT Policy Sector Guidelines* (2014).
[18] Section 2 (a) *ICT Policy Sector Guidelines* (2014).
[19] http://www.internetworldstats.com/africa.htm#ke on 5 January 2016.
[20] http://www.moseskemibaro.com/2014/08/01/sizing-up-twitter-in-kenya/ on 6 January 2016.
[21] http://www.whatsapp.com on 6 January 2016.

The legal and regulatory framework in Kenya is comprised of various laws and institutions that have been formulated and created to govern and regulate communication and cyberspace in general. This chapter looks at the general and specific framework, while conclusions and recommendations are made in the last chapter of this dissertation based on the analysis of the existing framework and comparison with other jurisdictions.

3.2 LEGAL FRAMEWORK

3.2.1 Constitution of Kenya 2010

The Constitution of Kenya is the supreme law of the land binding all persons and state organs at all levels of Government. [22] This means that no law is above the Constitution of Kenya. Chapter 4 of the Constitution provides for the bill of rights which provides for a basic outline of all rights and freedoms that Kenyans are entitled to. With regard to the constitutional provisions that apply to regulating cyberspace in general, there are several key provisions that govern the area in question. The freedom from discrimination, freedom of expression and the right of access to information are some of the fundamental rights and freedoms that form the framework on cyberspace that extend to cyberbullying and harassment.

The freedom from discrimination by the state or by individuals is an important freedom that is enforced by the constitution. The grounds of race, gender, pregnancy, marital status, health status, ethnicity, skin colour, age, disability, belief, dress, language among others form a base for discrimination which is protected against by the Constitution. [23] On most occasions, cyberbullying and harassment is formed on the basis of some form of discrimination with the actions addressed at attacking a certain dislike.[24] The Constitution helps address this by establishing provisions against discrimination in any form.

The freedom of expression is an important freedom in any mode or field of communication be it online or offline. This is provided for by the constitution which states that every person has the right to freedom of expression that includes seeking information, creativity and research.[25] However, with the freedom of expression being a fundamental freedom open to everyone under the constitution, there is a likelihood of misuse. This is covered by

[22] Article 2, *Constitution of Kenya* (2010).
[23] Article 27, *Constitution of Kenya* (2010).
[24] Beckerman, L., & Nocero, J, High-tech student hate mail; *The Education Digest (2003), 68*(6), 37-40.
[25] Article 33(1), *Constitution of Kenya* (2010).

the inclusion of a sub article that expressly states that it does not extend to *"propaganda for war, incitement to violence, hate speech or advocacy of hatred that either constitutes ethnic incitement, vilification of others or incitement to cause harm, or is based on any ground of discrimination."*[26] In exercising this right, people are also required to respect the rights and reputation of others. [27]

Access to information is an important right established by the constitution.[28] Persons have the right to access information online or offline while respecting the right to privacy. Further, every person has the right to correction or deletion of untrue or misleading information that affects the person. The latter provision ensures that the reputation of other people is protected and that information in the open is accurate and does not mislead anyone.

Should citizens feel that their rights have been impeded, the constitution provides for the right to access justice in a manner that does not impede its access or its delay[29]. Justice is important in establishing a working system where citizens of Kenya can enforce action where need be and have the law applied in totality.

In addition to bearing key provisions for fundamental rights and freedoms, the Constitution also enforces limitations to these rights and freedoms.[30] However, when one of these rights is limited, it can only be limited by law and only to the extent that the limitation is reasonable and justifiable in an open and democratic society. This has to also take into account factors such as the nature of the right, importance of the limitation, extent and nature of the limitation, the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights of others and whether there are less restrictive means to achieve the purpose. This is important to ensure that certain freedoms and rights can be limited when necessary, for example in ensuring public safety.

The constitution serves as the highest law regulating cyberbullying and harassment under the above provisions in Kenya. However, being a piece of legislation, this dissertation will look at how well it is being enforced in regulating against cyberbullying and harassment in the country.

---

[26] Article 33, (2), *Constitution of Kenya* (2010).
[27] Article 33, (3), *Constitution of Kenya*(2010).
[28] Article 35, *Constitution of Kenya* (2010).
[29] Article 48, *Constitution of Kenya* (2010).
[30] Article 24, *Constitution of Kenya* (2010).

3.2.2 The Kenya Information and Communication Amendment Act 2013

The Kenya Information Communication Amendment Act 2013 was assented in December 2013 and commenced in January 2014, having been enacted to amend the Kenya Information and Communications Act, 1998, Cap 411[31]. Cap 411 A has 7 parts covering a broad range of modes of communication such as radio, post and other modes of broadcast. The specific regulation forming part of the Kenyan framework being investigated by this study is part VIA which instructs on Electronic Transactions.[32] It enunciates the role of the Communication Authority in facilitating electronic transactions for ease of communication. A large part of the sections contained in Part VIA deal with electronic fraud, electronic records and signatures and unauthorized access to data.[33] The closest regulation that the Act comes to tackling cyber related offences specifically cyberbullying and harassment is Section 84D that deals with Publishing of obscene information in electronic form. The act subjects to conviction for a term not exceeding two years or a fine not exceeding two hundred thousand shillings a *person who transmits or causes publishing in electronic form of material deemed to be lascivious or appealing to the prunient interest whose effect is to deprave and corrupt persons likely to read, see or hear the matter embodied therein.* [34]The Act does not expressly mention or refer to cyberbullying or harassment in any way but mentions enablers such as computer systems that pave the way for bullying and harassment to occur online.

3.2.3 Cybercrime and Computer Related Crimes Bill 2014

Kenya has never had a cybercrime bill and owing to the technological advancements that have marked the 21st Century as recognised in the ICT Policy, there has been a need to create a legal regime that addresses and tackles cybercrime as part of effort to regulate cyberspace. As a result, a draft cybercrime bill had to be introduced which is at the time of writing being discussed before it passes into law. The Bill is an initiative of the Office of the Director of Public Prosecutions which is responsible for overseeing criminal prosecutions in Kenya. It came as a realisation that Kenya needs to tackle cybercrime which was estimated to have cost Kenya nearly 2 billion shillings in 2013 and also from the pressure of a cybersecurity conference in 2014 where there was pressure to have the

[31] Foreword, *Kenya Information and Communications* (Amendment) Act, (2013).
[32] Part VIA, *Kenya Information and Communication Act* (Cap 411A).
[33] Sections 83, *Kenya Information and Communication Act* (Cap 411A).
[34] Section 84D, *Kenya Information and Communication Act* (Cap 411A).

private sector involved in tackling cybercrime and related offences. [35] The Draft Bill has sections on offences against confidentiality, integrity of computer data and systems[36], access with intent to commit offences[37], computer related offences[38], content related offences such as hate speech and cyber stalking[39], procedures and investigations[40] and general penalties[41].

The Bill seeks to address cybercrime and related offences by staying in consistency with the Cybercrime Convention. With particular regard to this dissertation, the following sections of the Bill are deemed to be part of the framework regulating against cyberbullying and harassment. Section 18 classifies the offence of cyberstalking as a content related offence. The Bill states that a person who *wilfully, maliciously and repeatedly uses a computer system including electronic communication to harass, intimidate or cause substantial emotional distress or anxiety to another person, makes a threat withy an intention to place a person in reasonable fear, communicates obscene, vulgar, profound or indecent language, picture or image, displays or distributes information in a manner likely to increase the risk of harm to another person, is liable to a fine of three hundred thousand Kenya Shillings or imprisonment of three years.* It addresses harassment and includes even unconsented image distribution as an offence. In addition to this, hate speech can also be tied in as a form of harassment classified through the words of section 16 that state that a person using threatening, abusive or insulting words, displaying, publishing or distributing any written or electronic material through a computer system which is threatening, abusive or insulting is an offence if the person intends to stir up hatred. It's also immaterial whether the offence is committed publicly or privately. This section particularly gives reference to ethnic hatred. However, this is not the only probable offence that can be stirred by hate speech.

In addition to criminalising offences in the aforementioned sections, the Draft Bill addresses procedural ways to prosecute such offences. Gathering evidence and building up a case in cyberspace can have its challenges and one of them being disclosure of data.

---

[35] Article 19, Legal Analysis of the Draft Kenya Cybercrime Bill (2014), 6.
[36] Section 3, *Draft Cybercrime Bill of Kenya* (2014).
[37] Section 4(1), *Cybercrime Bill of Kenya* (2014).
[38] Part III, *Cybercrime Bill of Kenya* (2014).
[39] Sections 17, 19, *Cybercrime Bill of Kenya* (2014).
[40] Part V, *Cybercrime Bill of Kenya* (2014).
[41] Section 4, *Cybercrime Bill of Kenya* (2014).

Disclosure is important for prosecutors to build a case but it has its challenges based on the fact that at times, data being collected may be in outside jurisdictions[42] The Draft Bill encompasses disclosure of data as an important part to prosecution of cybercrime and related offences. It gives a police officer or a lawful authority, the authority to apply to a court of law for an order of the disclosure of data stored or processed by means of a computer system or any other information and communication technology and sufficient data to identify service providers and the path through which the data was transmitted.[43] This has the intention to help prosecutions without there being unlawful interference of privacy. The question of jurisdiction is also covered by the Draft Bill where an act committed or omitted under the Bill in Kenya, by a national of Kenya outside Kenya, on a ship or aircraft registered in Kenya, using a Kenyan domain name and outside Kenyan territory where the result of the offence has an effect in Kenya.[44] However this broad provision poses a challenge in prosecution of offences outside the country as well as getting information necessary for prosecution where the information is held in other jurisdictions.

3.3 INSTITUTIONS

The framework is also composed of institutions that have the mandate of enforcing the regulations prescribed by statutes and any other mandate conferred upon them by law.

3.3.1 Ministry of ICT

The Ministry of Information Communication and Technology in Kenya is responsible as the main authority overseeing communication and technology in Kenya as well as general policy formulation. [45] The Ministry has the general mandate of ensuring communication laws are well laid out and information is well distributed and every citizen has the right to access information in tandem with the Constitution of Kenya. The Ministry has made a key contribution to the general ICT field in Kenya by publishing the Draft National ICT Policy in 2006 that has been crucial in steering Kenya's goals in the ICT field and among them to enact cybersecurity laws which has the aim of creating a society that can thrive on ICT to

---

[42] House of Lords Select Committee on Communications, Social Media and Criminal Offences, 2014-2015.
[43] Section 27, Draft Cybercrime Bill of Kenya (2014).
[44] Section 35, Draft Cybercrime Bill of Kenya (2014).
[45] http://www.information.go.ke/?p=496 on 6 January 2016.

improve the livelihood of Kenyans. [46] In addition to this, the Ministry has played a particularly important role in overseeing implementation of cybersecurity in East Africa and beyond by hosting the Second Annual East Africa IT and Cyber Security Convention that brought together African leaders to determine new measures to ensure security in cyberspace in 2012.[47]

3.3.2 The Communication Authority

Formerly known as The Communications Commission of Kenya, (CCK), the Communication Authority is the regulatory body for communication in the country. It was established in 1998 by the Kenya Information and Communications Act and tasked with facilitating and developing the information and communication sectors in Kenya. Among its main responsibilities such as licensing, the authority also regulates communication services and monitors communication while facilitating access to communication and information as is required by the constitution.[48]The Communications Authority has the mandate to provide an updated database of communication laws to the public. This ensures that the citizens are kept in the know on the law. It forms a large part of the general framework governing communications in the country.

This is the current framework in Kenya regulating the whole communication and cyberspace sector. Whether this framework is enough to protect against cyberbullying and harassment in Kenya remains to be seen and will be analysed in the last parts of this dissertation.

3.3.3 Office of the DPP

The Office of the Director of Public Prosecutions deals is responsible for undertaking public prosecutions in Kenya. It deals with matters of harassment as offences to the person and treats them as human rights violations prosecuted by the Human Rights and Judicial review Division[49]

---

[46] http://www.information.go.ke/?p=496 on 6 January 2016.
[47] http://www.information.go.ke/?p=383 on 6 January 2016.
[48] http://www.ca.go.ke/index.php/what-we-do on 7 January 2016.
[49] http://www.odpp.go.ke/index.php/human-rights-and-judicial-review-division.html on 9 January 2016.

CHAPTER 4: COMPARATIVE ANALYSIS

This Chapter encompasses the application of other jurisdictions in the matter seeking to be addressed in this dissertation. One of the ways in which laws are made more cohesive is through borrowing from other jurisdictions and assessing how effective some of their laws are. This will be no different and will seek to analyse some key jurisdictions that Kenya may borrow from so as to strengthen the present legislation. The United Kingdom, South Africa and Tanzania will form the base for this analysis. These jurisdictions have been chosen based on the rationale that they are all related to Kenya in different ways. For instance, most of Kenya's laws are moulded under common law while South African and Tanzania are African countries that closely compare to Kenya in the Internet development field and therefore make good reference for comparison. The comparative analysis will be gauged on several elements, namely: What is the existing framework? How does the existing framework work? What have its successes been? Does it have loopholes? What Kenya can borrow from the existing framework in the different countries will serve as recommendations in the subsequent chapter.

4.1 THE UNITED KINGDOM

The English enjoy a rich history of common law. Dating as far back as the early 1800's, Parliament enjoyed the legislative role and had a huge part to play in the development of laws. Aspects of policing were present from as far back as 1847 for England, Wales and Scotland as seen through the Town Police Clauses Act. The existence of these laws has come a long way in the formulation of a legal framework by the UK. For this comparative analysis, the focus is on communication laws.

Communication laws have been present in the UK for a couple of years. The two main communication acts currently in the UK form a major part of the regulatory framework, i.e The Malicious Communications Act of 1998 of 1988 and the Communications Act of 2003. They both cover a wide range of communications from electronic communication to print communications. For this chapter, the focus will be on the regulation of electronic communication as it is the most relevant to the matter addressed in this dissertation. The Communications Act of 2003 makes a clear definition of Electronic communications networks and services as the means of relaying information through electronic means. Electronic Communications Services refers to a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of

signals, except in so far as it is a content service.[50] It then goes on to make improper use of electronic communications an offence in section 127. *A person is guilty of an offence if he sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent.*[51] *A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he sends by means of a public electronic communications network, a message that he knows to be false, causes such a message to be sent; or persistently makes use of a public electronic communications network.*[52]In addition to having these two clauses, the act imposes a penalty for the above offences. It lists summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both as the punishment if one is found liable for the listed offences[53] The Malicious Communications Act on the other hand creates offences for electronic communications which are indecent or grossly offensive, convey a false threat, provided that there is an intention to cause distress or anxiety to the victim.[54] These two acts are the main acts used to prosecute electronic communication offences.

Another piece of legislation that is suited to providing the framework for electronic offences in the UK is the Protection from Harassment Act of 1997. Harassment is a key part of cyberbullying and cyber harassment and this legislation aims to cover harassment as a communication offence targeting individuals. The Act protects victims from harassment, stalking, stalking involving fear or violence and harassment causing serious alarm or distress. [55] From the above pieces of legislation, it is clear that the acts of cyberbullying and harassment are treated as a criminal offence. Further, when electronic communication and social media facilitates a platform for defamation, it is dealt with in a different way by being privately actionable in the High Court with damages as a remedy to the injured party.

As part of the regulatory framework, the Director of Public Prosecutions in the UK instituted several consultations that were to form a guideline to social media and related

---

[50] Section 32 (2), *Communications Act* (UK) (2003).
[51] Section 127 (1), *Communications Act* (UK) (2003).
[52] Section 127 (2), *Communications Act* (UK) (2003).
[53] Section 127 (3), *Communications Act* (UK) (2003).
[54] Section 1, *Malicious Communications Act* (UK) (1988).
[55] Sections 2 &4, *Protection from Harassment Act* (UK) (1997).

offences. This sought to give the Crown Prosecution Service, which is the principal prosecution authority for England and Wales acting independently in criminal cases investigated by the police[56], the mandate to carry out prosecution in cases involving communications sent via social media. In setting out these guidelines, prosecutors are required to only start a prosecution if they command a two stage test called the Full Code Test.[57] The test has two stages, the evidential stage where prosecutors are required to consider whether there is sufficient evidence for a realistic prospect of conviction. The second stage is the public interest stage where no prosecution should be brought forward unless it can be shown on its own merits and facts to be both necessary and proportionate. Usually, a prosecution matter is unlikely to be both necessary and proportionate where:

i. The suspect has swiftly taken action to remove the communication or expressed genuine remorse;

ii. Swift and effective action has been taken by others for example, service providers, to remove the communication in question or otherwise block access to it;

iii. The communication was not intended for a wide audience, nor was that the obvious consequence of sending the communication; particularly where the intended audience did not include the victim or target of the communication in question; or

iv. The content of the communication did not obviously go beyond what could conceivably be tolerable or acceptable in an open and diverse society which upholds and respects freedom of expression.[58]

This has set a debate for the high threshold of prosecuting such crimes and setting a balance between the freedom of speech protected by Article 10 of the European Convention on Human Rights. Article 10 protects not only speech which is well-received and popular, but also speech which is offensive, shocking or disturbing. Precedent also indicates an attempt to bring in the discussion on the freedom of expression in attaining a threshold for prosecuting such cases.[59]

---

[56] http://www.cps.gov.uk/ on 8 January 2016.
[57] http://www.cps.gov.uk/consultations/social_media_consultation.html, Guideline 5, on 8 January 2016.
[58] http://www.cps.gov.uk/consultations/social_media_consultation.html, paragraph 39, on 8 January 2016.
[59] *Sunday Times v UK* (No 2) [1992] 14 EHRR 123.

Despite this debate, there have been successful convictions using the applicable laws and the authorities. Cases on abuse to a black footballer, Fabrice Muamba, who had collapsed on the pitch, abusive tweets to a person campaigning for a woman's face to appear on a banknote, among others have been investigated and prosecuted in recent years.[60] Perhaps Kenya ought to borrow from the UK system and amend/create laws to facilitate the punishment of such offences as they continue increasing?

4.2 TANZANIA

The United Republic of Tanzania is a growing nation neighbouring Kenya to the south. For most parts of the previous decades, the two countries have been toe to toe in terms of development and trade among other aspects. On the ICT field, Tanzania has almost 7.6 million internet users, being almost four times less the number of Kenyan internet users.[61] This number has been steadily increasing over the years and is expected to grow even higher with the rising accessibility to the internet.

Communication is regulated by the Tanzania Communications Regulatory Authority (TCRA) which serves almost a similar function as the CA here in Kenya. There are several relevant statutes in Tanzania responsible for regulating communications and specifically electronic communications. The Electronic and Postal Communications Act of 2010 was enacted to deal with regulation of communication systems including both electronic and postal communications. Regard to electronic communications is given by Part II and VI with the respective parts dealing with licensing and access, and offences respectively. Persons who use network facilities, services, application services, content services to transmit, request, suggest communication that is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person are liable to a punishment of a fine of not less than 5 million Tanzanian Shillings or imprisonment of a term not less than 12 months or both[62]. This is almost similar to the UK stand on improper use of electronic communications. The real test however comes in when qualifying what is offensive in character, what is abusive and whether it threatens or harasses a person. All these elements have to come together for there to be an offence. That has been a challenge in establishing what constitutes cyber harassment or cyberbullying.

---

[60] House of Lords Select Committee on Communications, Social Media and Criminal Offences, 2014-2015.

[61] http://www.internetworldstats.com/africa.htm#tz on 5 January 2016.

[62] Section 118, *Electronic and Postal Communications Act* (Tanzania) (2010).

In 2013, Tanzania realised the need to create laws governing cyberspace following several credible threats from cybercrime in general such as cyber related fraud and harassment online. There were increased calls on the legislators and the government in general to enact laws protecting internet users. Despite the TRCA's efforts to educate people on using the internet, it was not enough. It was during the first cybercrime conference held in Dar Es Salaam that there were promises to enact laws tackling cybercrime.[63] This need to legislate against cybercrimes saw the drafting of the Cybercrime Bill which has since become law after parliament passed it. The Cybercrime Act applies to Mainland Tanzania as well as Zanzibar. Part II of the Cybercrime Act is committed to dealing with offences and penalties for crimes such as computer related forgery, data espionage, genocide and cyberbullying. In particular regard to cyberbullying, a person is not allowed to initiate or send any electronic communication using a computer system to another person with intent to coerce, intimidate, harass or cause emotional distress. If this happens, the person is liable to a fine of not less than three million shillings (equivalent to 140,000 Kenya Shillings) or imprisonment for a term of not less than one year or both. [64] The act does well at listing cyberbullying as an offence but fails to factor in the fact that cyberbullying can be conducted through mobile phones which are the most common way of accessing the internet with the growing number of mobile subscribers. In addition to this, the Act doesn't serve to demystify most definitions in Section 2 which would be a crucial part to understanding and covering loopholes in the cybercrime field.

Despite these minor issues in the legal framework, Tanzania has done a good job at enacting laws that attempt to combat cybercrime in the country and has set good precedent for other countries to follow. Kenya could definitely borrow a leaf from the Southern neighbours.

4.3 SOUTH AFRICA

South Africa is considered to be one of the most technologically advanced countries in Africa with an internet penetration percentage of 49% and 8% of internet users in the country. It falls 4th in Africa among Africa's top 10 internet countries at 26.8%.[65] Further

[63] http://allafrica.com/stories/201409140013.html on 6 January 2016.
[64] Section 23, *Cybercrime Act* (Tanzania) (2015).
[65] http://www.internetworldstats.com/stats1.htm on 5 January 2016.

comparative data indicates that South Africans are one of the highest users of mobile technology and mobile social networking on the continent compared to other countries like Tanzania, Zambia and Ethiopia. [66]

The framework in South Africa is composed of institutions as well as statutes. The South Africa Electronics Communications and Transactions Act commits Chapter XIII to cybercrime listing its definition and offences of unauthorised access, computer related extortion, fraud and aiding and abetting. [67] Chapter XII formulates Cyber inspectors whose powers include monitoring any websites or activities on an information system, inspection, among others.[68]

Much like Kenya, South Africa has no Cybercrime Act yet, however, a bill is in place to regulate against cybercrimes. Chapter 2 of the Cybercrimes and Cybersecurity Bill of 2015 lists definitions and offences covered under the Bill. There is no direct mention of cyberbullying and harassment but its aspects are alluded to by Section 17 which prohibits dissemination of data messages which advocate, promote or incite hatred, discrimination and violence. Chapter 4 of the Bill discusses investigations, search and access or seizing. There is provision for disclosure of data to aid investigations[69] as well as prohibition on disclosure of information[70] which is a key part of the framework against cyberbullying and harassment. Chapter 5 and 6 form the institutional breakdown for cybercrime and cybersecurity. A 24/7 point of contact is established[71] where policing is encouraged and administration by cybersecurity experts. In addition to this, Chapter 6 proposes structures to deal with cybersecurity among them a Cyber Response Committee, Cyber Security Centre, Government Security Incident Response Team, National Cybercrime Centre, Cyber Command Centre and a Cyber Security Hub. All of these structures have different but interlinked functions. The Bill seeks to create an important change in how cybersecurity in general is handled in South Africa.

---

[66] Berger G & Akshay S, South African mobile generation: A study on South African young people on mobiles. UNICEF NY, *Division of Communication, Social and Civic Media Section* (2012).
[67] Sections 85-89, *Electronic Communications and Transactions Act* (South Africa) (2002).
[68] Section 81, *Electronic Communications and Transactions Act* (South Africa) (2002).
[69] Section 41, *Cybercrime and Cybersecurity Bill* (South Africa) (2015).
[70] Section 38, *Cybercrime and Cybersecurity Bill* (South Africa) (2015).
[71] Section 49, *Cybercrime and Cybersecurity Bill* (South Africa) (2015).

Aside from statutes, South Africa has a Department of Communications that formulates policies and reforms in the Communications Sector. In dealing with cyberbullying and harassment, the Department of Communications is working on a Children and ICT strategy aimed at protecting children in the ICT sector while recognising the need to prevent crimes such as child pornography and cyberbullying which have a reputation of being notorious among children. [72] There are also online resources that serve as communication database centres for South Africans to read on cyberbullying and learn how to tackle and handle it. *Cyberbullying.org.za* is a main resource centre established by the Centre for Justice and Crime Prevention (CJCP) to act as a resource centre for internet safety and cyberbullying in South Africa. [73]

4.4 FINDINGS

The findings of this chapter are drawn from a comparative analysis of the United Kingdom, Tanzania and the South African context analysed with the third chapter of this study.

Kenya's legal framework lacks a specific legislation to combat cyberbullying and harassment online. Based on the case study of the Kenyan context, the laws in Kenya only come close to the problem but do not tackle the problem in totality. This is evidenced by the operational law statute which is the Kenya Information and Communications Act. The Act has been subject to amendments from time to time with the latest one being in 2013 but has not yet tackled the question of criminalising or regulating against cyberbullying and online harassment. Currently, under the Act, publishing of obscene information in electronic form incurring a penalty of a fine not exceeding two hundred thousand Kenya Shillings and an imprisonment term of 2 years is the relatable offence that comes close to tackling harassment and bullying.[74] This means that if there is to be a case taken forward to the Courts involving online bullying and harassment, the courts would not have a specific law to prosecute the offence accurately. This is however being remedied by the proposed Cybercrime Bill to create a framework for analysing cybercrime.

The Cybercrime Bill of 2014 is a positive step for Kenya in tackling online harassment and bullying. However, when compared to the current Tanzania Cybercrime Act and the South

[72] Masa Popovac &Lezanne Leoschut, Cyberbullying in South Africa, Impact and Responses, *CJCP Issue Paper No. 13* (June 2012).
[73] http://www.cyberbullying.org.za/ on 8 January 2016.
[74] Section 84D, Kenya Information and Communication Act Cap 411A.

African Cybercrime Bill, it fails to meet the high standard set. Tanzania has an established clause on Cyberbullying that forbids a person from initiating or sending any electronic communication using a computer system to another person with intent to coerce, intimidate, harass or cause emotional distress.[75] This provision however fails to meet the dynamic nature of online harassment and bullying. It does not capture the definition of what cyberbullying is and it only gives regard to a computer system yet mobile phones can also be used to bully or harass since they offer access to the internet and social media sites through mobile data. An amendment to this provision would be in order, however, the effort made by Tanzania is commendable. In comparison to South Africa, Kenya's Cybercrime Bill appears inferior in regulating and providing reporting mechanisms for victims of harassment and Cyberbullying. The Cybercrime Bill of South Africa 2015 provides for investigations to be conducted and disclosure of data when offences under the Bill occur. The major difference between the Kenyan Bill and the South African Bill is evidenced in Chapter 6 of the South African Bill. The Bill provides for the establishment of 24/7 contact centres, a Cyber Response Committee, Cyber Security Centre, Government Security Incident Response Team, National Cybercrime Centre, Cyber Command Centre and a Cyber Security Hub all with different roles in a bid to strengthen the grip on cybersecurity. In addition to this, there is the Centre for Justice and Crime Prevention that provides for a specific information resource database on Internet safety which is not under the Bill as it is already operational. Kenya's Bill on the other hand does not provide for establishment of any centres tailored to deal with cybercrime despite being the leading authority on cybercrime. Borrowing from the South African Cybercrime Bill could go a long way in improving the framework on cybercrime in Kenya.

The Office of the Director of Public Prosecutions (O.D.P.P) is not adequately specialised in dealing with cybercrimes yet. The Human Rights and Judicial Review Division deals with cases of harassment as crimes against a person and as a human rights violation. There is no specialised division yet to tackle cyber related offences. This shows the inadequacies of the Cybercrime Bill in not creating a specialised unit. Prosecutions form a key part of the efforts to regulate against cybercrime and this therefore needs to be reflected in the D.P.P's office much like the United Kingdom where the CPS undertakes independent investigations from the police using the Full Code Test.

---

[75] Section 23 *Cybercrime Act* (Tanzania) (2015).

CHAPTER 5: RECOMMENDATIONS TO THE KENYAN FRAMEWORK

Cyberbullying and harassment is a current and emerging issue arising from technology advancement. There is a recognised framework in Kenya governing communication in general but does it narrow down to the specifics that this dissertation seeks to address? This remains to be seen, however, one thing is certain, that there is more to be done to improve the law that addresses the problem at hand. This chapter will propose recommendations that are necessary for the improvement of the existing framework as well as other general recommendations that can help solve the issue of cyberbullying and harassment.

5.1 Amendments to the Cybercrime Bill of 2014

Being a relatively new Bill, there is room to make it fundamentally stronger than it is. Cyberbullying and harassment has no specific provision yet as is the case in Tanzania's Cybercrime Act.[76] However, harassment is tackled under Section 18 which regulates against Cyberstalking bordering on the violation of the right to privacy online. The inclusion of a specific clause/section regulating against cyberbullying to include harassment and stalking as part of it should be carried out to provide for a stronger provision. In addition to this, the Bill should create institutions to deal with cybersecurity as a whole which should then deal with cyberbullying as a part of cybercrime. This can be borrowed from South Africa's Draft Bill on Cybercrime and Cybersecurity.

5.2 Reforming the Cybercrime Division in policing

The prevalence of cybercrime has seen Kenya lose a lot of money through fraud and other related offences.[77] Perhaps it would be best if there was a specific division in the Police Administration dealing with cybercrime and related offences as a specific crime. There is said to be an existing Cybercrime Unit within the Kenya police. However, little is known about the unit and the prosecutions that it has spearheaded so far. This particular division ought to be composed of specialists in cybercrime to ensure competency and proper understanding of cyber security laws for subsequent implementation and prosecution. Borrowing from South Africa, there are cyber inspectors who have the duty to monitor and inspect websites or activity on an information system and report any unlawful activity to

[76] Section 23, Cybercrime Act Tanzania (2015).
[77] Article 19, Legal Analysis of the Draft Kenya Cybercrime Bill (2014),6.

the appropriate authority.[78] Kenya could borrow from the South African model of cyber inspection to monitor and deal with events of cyberbullying and harassment especially on social media. Having a specialised unit will also have more emphasis placed on the regulation and monitoring cyberbullying and harassment and in extension, the regulation and prevention of cybercrimes in the country. Borrowing from the Cybercrime Bill of South Africa, this could also go hand in hand with instituting specific provisions in the Cybercrime Bill that establish specialised Cybercrime Units and list its functions and powers for Kenyans to be informed on.

5.3 Elaborate Guidance of Prosecution in D.P.P's office

The office of the Director of Public Prosecution responsible for conducting public prosecution should be well equipped and staffed with competent prosecutors who are well versed with cyber related offences. This can best be done through a guidance of prosecution for such offences to ensure that prosecutions are carried out in the right way and the right procedure is followed.[79] This can be borrowed from the United Kingdom's model of the Crown Prosecution Service where prosecutors are required to follow the full code test. The test ensures that evidence is sufficient enough to conduct a prosecution and that the prosecution is both necessary and appropriate.[80]

5.4 Facilitating education and creating awareness

This should be the first step to solidifying the efforts to regulate against cyberbullying and harassment on social media. It applies to different parties, among them, children, adults and police. Education can start from schools to teach children how to deal with cyberbullies they encounter online and how to use social media for good. This can be done through digital safety programs in schools aimed at young people[81]. In addition to this, parents need to be provided with knowledge and practical knowhow to understand the merits and demerits of online engagement. This will help curtail the likelihood of their children engaging in misuse of digital media. As for prosecutors, there is a certain level of knowledge and skill required to display at the top level. However, due to the dynamic

---

[78] Section 81, Electronics Communications and Transactions Act South Africa (2002).
[79] The Prosecution of Offences Act, United Kingdom (1985).
[80] http://www.cps.gov.uk/consultations/social_media_consultation.html, Guideline 5, on January 8th 2016.
[81] UNICEF, A (Private) Public Space, Examining the Use and Impact of Digital and Social Media Among Adolescents in Kenya (2013).

nature of technology, they need to enrich their education to equip themselves with adequate information suitable to initiate and execute a prosecution.

Campaigns are an effective way of spreading awareness. South Africa has undertaken campaigns in its internet safety policy as a way of educating its people on the dangers of internet safety. These campaigns should also teach and advise internet users on how to adopt security safety measures while networking on social media sites. Most of the social networks, (Facebook and Twitter have dedicated Terms of Service and Privacy policies) have privacy policies that allow for blocking and reporting of other users who are a threat to their privacy and safety.

5.5 Conclusion

Drawing from the findings of the analysis of the Kenyan context and the subsequent comparative analysis of the Jurisdictions, this study shows that indeed the framework in Kenya contains a myriad of loopholes that need to be attended to in order to deal with the issues of cyberbullying and harassment effectively for the present and the future.

There is a lot that Kenya can borrow from other jurisdictions out there to deal with this issue. The capacity to do so is present and attention should be given by the legislature to improve on the existing framework. Further, this should be treated as a crime and not as a tort. Criminal law will offer a wider reach of punishment as compared to civil law.

BIBLIOGRAPHY

Books

1. Robin M. Kowalski, Susan P. Limber, Patricia W. Agaston, *Cyberbullying: Bullying in the Digital Age* (2012).
2. John Stuart Mill, On Liberty (1859).

Reports

1. Communications Authority, 1st Quarter Sector Statistics Report for the Financial Year 2015-2016.
2. UNICEF, A (Private) Public Space, Examining the Use and Impact of Digital and Social Media Among Adolescents in Kenya (2013).
3. House of Lords Select Committee on Communications, Social Media and Criminal Offences, 2014-2015.
4. Berger G & Akshay S, South African mobile generation: A study on South African young people on mobiles. UNICEF NY, *Division of Communication, Social and Civic Media Section* (2012).
5. Masa Popovac &Lezanne Leoschut, Cyberbullying in South Africa, Impact and Responses, *CJCP Issue Paper No. 13* (June 2012).

Journal Articles

1. Campbell, Marilyn A (2005) Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling* 15(1):68-76.

Internet Sources

1. http://www.internetworldstats.com/stats.htm on 5 January 2016.
2. http://www.internetworldstats.com/africa.htm#ke on 5 January 2016.
3. http://www.moseskemibaro.com/2014/08/01/sizing-up-twitter-in-kenya/ on 5 January 2016.
4. http://www.whatsapp.com on 6 January 2016.
5. http://www.information.go.ke/?p=496 on 6 January 2016.
6. http://www.information.go.ke/?p=383 on 6 January 2016.
7. http://www.ca.go.ke/index.php/what-we-do on 7 January 2016.

8. http://www.odpp.go.ke/index.php/human-rights-and-judicial-review-division.html on 9 January 2016.
9. http://www.cps.gov.uk/consultations/social_media_consultation.html, Guideline 5, on 8 January 2016.
10. http://www.internetworldstats.com/africa.htm#tz on 5 January 2016.
11. http://allafrica.com/stories/201409140013.html on 6 January 2016.